HUMAN RIGHTS WATCH

Human Rights Watch Submission to the Department of Home Affairs Regarding the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

September 10, 2018

I. Summary

Human Rights Watch welcomes the opportunity to submit these comments regarding the exposure draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018. This submission supplements comments filed on behalf of an international coalition of civil society organizations, technology companies, and trade associations that Human Rights Watch has joined.

As we wrote to former Prime Minister Malcolm Turnbull on August 3, 2017, strong encryption built into private sector technology is the cornerstone of cybersecurity in the digital age.[1] It protects the data—and the human rights and security—of billions of Internet users worldwide against growing security threats to personal and financial data, critical infrastructure, and even government agency systems.

All governments have a legitimate interest in investigating crime and thwarting security threats. We commend the Australian government's efforts to ensure that new tools crafted to address these concerns do not create "systemic weaknesses or vulnerabilities" in the technology ordinary Australians rely on every day.

However, we believe the bill still poses considerable threats to cybersecurity and human rights, including freedom of expression and privacy. The bill's broadly drawn powers, coupled with ambiguously defined limitations, do not sufficiently prevent the government from introducing widespread security vulnerabilities in the global digital ecosystem. The bill's safeguards and limitations fall short of what is required by human rights law, and its oversight mechanisms are not adequate to ensure that the extraordinary powers it grants

[1] Letter from Elaine Pearson, Australia Director and Cynthia Wong, Senior Internet Researcher, Human Rights Watch, to Hon. Malcolm Turnbull MP, Prime Minister of Australia, August 3, 2017, https://www.hrw.org/news/2017/08/03/letter-prime-minister-turnbull-re-encryption-and-human-rights.

will not be abused. Finally, the bill would set a dangerous, though unintended, precedent regionally and worldwide.

We urge the Department of Home Affairs to withdraw the Assistance and Access Bill and craft an approach that meets the legitimate needs of law enforcement agencies while also protecting cybersecurity and human rights.

II. The bill would undermine strong encryption and cybersecurity

The bill creates a new framework for compelling assistance from a broad range of communications service providers, foreign and domestic, to access communications content and data that may be protected by encryption or other technical measures. Schedule 1 grants three new powers to law enforcement and security agencies to secure such assistance:

- **Technical Assistance Request (TAR)**: provides a legal basis on which communications providers can provide **voluntary assistance** to certain security and interception agencies.
- **Technical Assistance Notice (TAN)**: issued by the Director General of Security or the head of an interception agency to **compel** communications providers to give assistance they are ***already capable of providing*** (for example, to seek decryption where the provider holds the encryption key).
- **Technical Capability Notice (TCN)**: issued only by the Attorney General (at the request of the Director General of Security or the head of an interception agency) to **compel** communications providers to ***build a new capability*** to ensure it can provide assistance.

We commend the inclusion of Section 317ZG in the draft bill, which prohibits assistance or capability notices (TANs or TCNs) from requiring a provider to build or implement a "systemic" weakness or vulnerability into a form of electronic protection, and from preventing providers from fixing a "systemic" weakness or vulnerability. The Explanatory Document of the Assistance and Access Bill further states that the section "ensures that providers cannot be asked to implement or build so-called 'backdoors' into their products or services."[2]

However, the bill itself does not define "systemic" and provides too much discretion to agencies issuing assistance or capability notices to determine its contours. Such decisions

[2] Australian Department of Home Affairs, Assistance and Access Bill 2018 Explanatory Document (2018), p. 47.

are made in secret and not subject to prior, independent judicial authorization. Other broadly drawn provisions in the bill, along with vaguely defined limitations, also undermine the intent and effect of this safeguard.

For example, the seemingly non-exhaustive list of "acts or things" that an agency may compel a provider to do is overly broad, and includes:[3]

- removing electronic protections applied by the provider (for TARs and TANs);
- providing technical information about their systems, including potentially source code or other information that would enable an agency to uncover existing vulnerabilities;
- installing software provided by the agency, including potentially installing government spyware on a target device;
- modifying or substituting a service, including potentially by prompting an individual to install a government-modified software update;
- notifying agencies of changes to the provider's service or technology; and
- concealing the fact that something has been done covertly in the exercise of a power.

Many of these actions could potentially introduce vulnerabilities that have widespread effects on cybersecurity and human rights.

For example, agencies could require a service provider to use its software update system to install modified code that enables access to encrypted communications. However, this would undermine trust in routine software update channels. It might drive users to avoid software updates out of fear of intrusion, which would leave their devices less secure over time because they may not install necessary software fixes. Such a result would undermine cybersecurity broadly for users beyond the targets of an investigation.

Similarly, the bill also appears to contemplate the type of action the United States Federal Bureau of Investigation (FBI) demanded from Apple in 2016 when it sought to compel the company to help access an iPhone used by a perpetrator in the San Bernardino shooting.[4] Yet Apple challenged this demand precisely because it raised proportionality concerns, stating that "once created, the technique could be used over and over again, on any

[3] Section 317E. Though this list is exhaustive with respect to TCNs, another provision allows the Minister to add additional items to this list in the future.

[4] Cynthia Wong, "Apple's Standoff and Security for All," commentary, Human Rights Dispatch, February 18, 2016, https://www.hrw.org/news/2016/02/18/dispatches-apples-standoff-and-security-all.

number of devices."[5] This concern was also echoed by other companies, cybersecurity experts, and rights organizations that filed friend-of-the-court briefs in support of Apple's challenge, including the UN Special Rapporteur on freedom of expression.[6] Nothing in the bill appears to prevent such repeated use of a capability once it is created.

Compelling the creation or installation of new software to subvert encryption or other security protections creates additional risks that the software could be breached, stolen, and disseminated, with far-reaching consequences for cybersecurity.[7] Such an outcome is made more likely because the bill itself does not seem to impose limits on use or retention of specific software or capabilities developed under its authorities. These concerns are further compounded by Schedule 2 of the bill, which creates new warrants that enable agencies to hack devices and directly access data before it is encrypted.

As a result, security experts, including those working for service providers, may characterize many of the capabilities the bill may compel as "backdoors" or as preventing use of strong, end-to-end encryption, despite the assurances of Section 317ZG.

As discussed more fully in Section IV, the bill does require the Attorney General to consult with companies before issuing a technical capability notice. However, the bill appears to provide few safeguards if the Attorney General overrules or discounts industry concerns about whether a notice would cause systemic harm.

The bill should not be introduced unless it incorporates stronger safeguards against the creation of encryption backdoors and other threats to cybersecurity.

III. The bill's safeguards and limitations are insufficient to protect rights or prevent abuse

The UN High Commissioner for Human Rights (OHCHR) and the UN special rapporteur on freedom of opinion and expression have recognized the centrality of strong encryption to freedom of expression and the right to privacy in the digital age. In a 2017 resolution, the UN Human Rights Council encouraged business enterprises to adopt encryption to "secure

[5] Tim Cook, "A Message to Our Customers," Apple, February 16, 2016, https://www.apple.com/customer-letter/ (accessed September 6, 2018).

[6] See "Amicus Briefs in Support of Apple," Apple, press release, March 2, 2016, https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple/ (accessed September 6, 2018).

[7] See, for example, Scott Shane, Nicole Perlroth, and David E. Sanger, "Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core," *The New York Times*, November 12, 2017, https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html (accessed September 10, 2018).

and protect the confidentiality of digital communications," and called on states "not to interfere with the use of such technical solutions" and ensure any restrictions comply with their obligations under international human rights law.[8] Thus, any restrictions on encryption should be provided by law and be necessary and proportionate for a legitimate aim. To be proportionate, the measure should be the least intrusive measure that achieves the aim.

As drafted, the bill falls short of these human rights requirements.

To issue an assistance or capability notice (TAN or TCN) under the bill, the Attorney General or agency head must be satisfied that the assistance sought is reasonable, proportionate, practicable, and technically feasible.[9] The bill's explanatory document states that in deciding whether a notice meets these criteria, the decision-maker will consider the interests of the agency, the communications provider, and the wider public interests, including the impact on privacy, cybersecurity, and innocent third parties.[10] It also states that the agency should "engage in a dialogue" with a provider prior to issuing a capability notice and may consult with "other persons who have relevant experience and technical knowledge."[11]

On its face, this standard appears to fall short of the requirement of necessity and proportionality. But even if it were sufficient, its terms are not defined in the bill itself, nor is the explanatory guidance reflected in the text of the legislation. While the explanatory document lists factors the decision-maker "must" or "would need to" consider, the bill language itself does not impose many requirements.[12] For example, while the explanatory text says the decision maker should consider the availability of other means to achieve an agency's objective, the legislation does not require it, nor does it require agencies to pursue less intrusive measures when they are available and equally effective. In all, this leaves too much discretion to the Attorney General or other agency head to decide whether a measure may be justified.

As discussed in the previous section, the breadth of the actions security agencies may compel under the bill also raise proportionality concerns with respect to their impact on

[8] Human Rights Council, "The right to privacy in the digital age," Resolution 34/7, A/HRC/RES/34/7, para. 9.
[9] Sections 317P and 317V.
[10] Explanatory document, pp. 9-10.
[11] Explanatory document, p. 38.
[12] Ibid.

rights and cybersecurity. For example, the OHCHR noted the wide-ranging risks to security and to rights in assessing the US FBI's demands of Apple in the San Bernardino case:[13]

> Personal contacts and calendars, financial information and health data, and many other rightfully private information need to be protected from criminals, hackers and unscrupulous governments who may use them against people for the wrong reasons. In an age when we store so much of our personal and professional lives on our smart phones and other devices, how is it going to be possible to protect that information without fail-safe encryption systems?
>
> So, in essence, what we have here is an issue of proportionality: in order to possibly—but by no means certainly—gain extra information about the dreadful crime committed by Syed Rizwan Farook and his wife in San Bernardino, we may end up enabling a multitude of other crimes all across the world, including in the United States. The debate around encryption is too focused on one side of the security coin, in particular its potential use for criminal purposes in times of terrorism. The other side of the security coin, is that weakening encryption protections may bring even bigger dangers to national and international security.

Finally, the range of purposes for which agencies can seek assistance is too broadly drafted to include enforcing the criminal law and laws imposing "pecuniary penalties," assisting the enforcement of criminal laws in a foreign country, "protecting the public revenue," and safeguarding national security.[14] The bill does not limit use of requests or notices to serious crimes or significant pecuniary penalties, raising questions of whether the intrusiveness of the proposed measures can be justified in a given case, such as collecting fines or catching minor tax-evaders. Though the explanatory document states that these powers will not be used to pursue "small-scale administrative fines," this limitation is not reflected in the text of the bill.[15]

The bill should not be introduced without significant revision to ensure any restriction on encryption in a given case is truly necessary and proportionate.

---

[13] "Apple-FBI case could have serious global ramifications for human rights: Zeid," United Nations Office of the High Commissioner for Human Rights press release.

[14] Sections 317G, 317L, and 317T.

[15] Explanatory document p. 31.

IV. The bill provides insufficient transparency, oversight, and accountability

The bill does not provide sufficient transparency, oversight, or accountability mechanisms, raising acute concerns that it will be inadequate to detect, prevent, and remedy abuses of the broad powers it creates.

The Director General of Security, the chief officer of an interception agency, and the Attorney General can issue notices without prior judicial oversight. This diverges from the UK Investigatory Powers Act, which established a prior judicial review regime for certain powers and created an Investigatory Powers Commissioner for specific oversight.[16] No such prior judicial review or independent commissioner, however limited a check on security and law enforcement agencies, figures in Australia's bill.[17]

To the contrary, the Attorney General or agency head itself determines whether a notice is reasonable and proportionate.

The bill's explanatory document provides that "Australian courts will retain their inherent powers of judicial review of a decision of an agency head or the Attorney General to issue a notice. This ensures that affected persons have an avenue to challenge a decision so that the court can determine whether the decision was lawfully made."[18] But the document also expressly excludes a "merits review" of decisions taken to issue technical assistance or capacity notices, meaning an affected person cannot ask a tribunal to examine the correctness of a decision to issue a notice.[19] The courts' powers of judicial review only enable an examination of whether the decisions are made within the legal limits of the legislation. Given concerns that the legal limits are themselves insufficient to protect rights (discussed in section III), this leaves only very narrow grounds for challenge.

This shortcoming is exacerbated by the lack of notice and transparency around when agencies employ technical assistance and capability notices. Providers will be required to conceal the existence of any specific notice or request, and any action taken covertly by law enforcement. The bill makes it an offence to disclose such information without authorization, with only limited exceptions (for example, to seek legal advice) and no exception for disclosure in the public interest.[20] The prohibition on disclosure applies in all

[16] Investigatory Powers Act 2016, part 8, chapter 1.

[17] See Human Rights Watch, Written Evidence to the Joint Committee on the Draft Investigatory Powers Bill, January 7, 2016, https://www.hrw.org/news/2016/01/07/written-evidence-joint-committee-draft-investigatory-powers-bill.

[18] Explanatory document, p.11.

[19] Ibid., p. 41.

[20] Section 317ZF.

cases with no time limits, even in cases where disclosure would no longer jeopardize an investigation or threaten national security or public safety.

The bill also relies too heavily on industry as the guardians of the public interest and of individual Australians' security interests, due process, and right to privacy. The bill requires the Attorney General to consult with affected communications providers prior to issuing a technical capability notice, and providers may provide feedback on the proposed notice's reasonableness, proportionality, and technical feasibility.[21] However, if the Attorney General disagrees with a provider's assessment that the notice is not reasonable or if the provider declines to challenge the notice, it is unclear how other affected individuals may challenge the government's actions.

While the bill does provide for periodic reporting of the number of requests and notices issued, aggregated data is no substitute for individualized notice to people whose rights may be infringed. Without notice, it is difficult to envision how "affected persons," other than service providers, would even know to seek what limited judicial remedies are available under current law.

When coupled with the exclusion of administrative review, and the narrowed ability to seek judicial review of the decision making, the lack of notice and transparency raises serious concerns around accountability for the exercise of executive power and people's ability to vindicate their human rights. Given the extraordinarily intrusive nature of the actions agencies can compel, such limited remedies and oversight are insufficient to ensure the powers are not abused nor to ensure individuals can secure meaningful remedy.

The bill should not proceed unless it requires prior authorization by an independent judge, avenues to challenge a decision on the merits, and notice for affected individuals, which can be delayed until such notice would not pose a threat to security or jeopardize an ongoing investigation but still remain a viable means of challenging the law or any decision taken under it.

V. The bill will set a problematic precedent with global ramifications

If the Australian government adopts the approach in this bill, it will set a dangerous global precedent.

[21] Section 317W.

Australia's approach to encryption may be emulated by governments worldwide at a time when many states are currently debating their own encryption policies.[22] If the government compels global companies like Apple, Facebook, or Google to disclose source code, subvert software update systems to install spyware, or remove electronic protections, other governments will demand the same. International service providers and device makers will find it more difficult to resist similar orders from both democratic and authoritarian regimes. The result will degrade protections for rights and damage cybersecurity far beyond Australia's borders.

Moreover, once Australia enacts such permissive legislation, many other countries with which it regularly conducts law enforcement cooperation may well funnel their requests through the government's existing cooperation mechanisms, given the global and interwoven nature of communications via the internet. This would place undue burden on the government and taxpayers of Australia and lower privacy and due process protections globally.

VI. Conclusion

Technology companies face an escalating digital arms race to secure their software and devices against cybercriminals and other digital threats, and encryption is a key part of their arsenal. Despite assurances that new powers will not introduce systemic weaknesses or vulnerabilities, the bill poses considerable threats to cybersecurity and human rights. If the Australian government pursues this approach, many other countries may follow suit, degrading security and rights on a global scale. We urge the Australian government to lead by example by adapting to a world with strong encryption instead of fighting the gains the private sector has made in shoring up protections for our data and devices in the digital age.

[22] See United Nations Special Rapporteur on the right to freedom of opinion and expression, *Encryption and Anonymity Follow-Up Report*, June 2018, https://freedex.org/wp-content/blogs.dir/2015/files/2018/07/EncryptionAnonymityFollowUpReport.pdf (accessed September 10, 2018.